UNITED STATES DISTRICT COURT FOR THE

DISTRICT OF MASSACHUSETTS

HOME MARKET FOODS, INC., Plaintiff, v. SCOTT LUBOW, Defendant.	C.A. No._____ **JURY TRIAL DEMANDED**

VERIFIED COMPLAINT FOR INJUNCTIVE AND EQUITABLE RELIEF

INTRODUCTION

1. Plaintiff Home Market Foods, Inc. ("**HMF**" or the "**Company**") brings this action against Defendant Scott Lubow ("**Mr. Lubow**"), a former highly-compensated HMF employee, for breach of his Non-Disclosure, Inventions, Work-For-Hire and Non-Competition Agreement (the "**Confidentiality Agreement**") and misappropriation of HMF's confidential information and trade secrets ("**Proprietary Information**"). Specifically, despite repeated requests from HMF, Mr. Lubow withheld returning HMF property—two HMF laptops issued for Mr. Lubow's use during his employment—for weeks following the termination of his employment. After his employment termination, Mr. Lubow unlawfully accessed HMF's Proprietary Information—including highly sensitive pricing, financial, and shipping information—residing on at least one of those laptops by inserting seven (7) different universal serial bus ("**USB**") drives into the laptop. HMF would be irreparably harmed if its Proprietary Information were provided by Mr. Lubow to an HMF competitor or customer. In particular, this information would allow a competitor to undermine HMF's sales and marketing efforts and unfairly compete with HMF for "shelf space" in the highly competitive Consumer Packaged Goods industry. Concomitantly,

disclosure of the Proprietary Information to HMF's customers would irreparably harm HMF's substantial goodwill and well-earned reputation in the industry—which HMF has spent many years cultivating and protecting. Mr. Lubow must not be allowed to disclose, transfer to, or provide anyone with HMF's Proprietary Information; but rather, he should be enjoined from doing so and compelled to return the information to HMF.

THE PARTIES

2. Plaintiff Home Market Foods, Inc. is a Massachusetts corporation with a principal place of business in Norwood, Massachusetts.

3. Defendant Scott Lubow is an individual residing in Lakeville, Minnesota.

JURISDICTION AND VENUE

4. This Court has original jurisdiction over this action pursuant to 28 U.S.C. § 1332, because the parties are citizens of different states and the value of the injunctive and equitable relief sought well exceeds the sum of $75,000. Among other things, HMF has spent millions of dollars over the years and upwards to $500,000 annually to protect its Proprietary Information.

5. Exercise of personal jurisdiction over Mr. Lubow is proper because, throughout the course of his employment with HMF, Mr. Lubow traveled regularly to the Company's Massachusetts headquarters for business meetings, had daily communications with HMF employees based in Massachusetts, and received paychecks issued from HMF from Massachusetts. As such, Mr. Lubow has sufficient minimum contacts with Massachusetts such that exercising jurisdiction over him does not offend traditional notions of fair play and substantial justice. Also, Massachusetts has a significant interest in providing a convenient forum for disputes involving its citizens and in ensuring that they have easy access to a forum when their contracts are breached by out-of-state defendants.

6. This Court also has original jurisdiction over this action pursuant to 28 U.S.C. § 1331 in that HMF asserts a claim for violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. This Court may exercise supplemental jurisdiction over HMF's state-law claims as they arise from a common nucleus of operative fact as the federal claim asserted.

7. Venue is appropriate in this judicial district under 28 U.S.C. § 1391(b)(3) because Mr. Lubow is subject to personal jurisdiction in this district. Also, Mr. Lubow consented to this venue as a proper venue pursuant to the express terms of the Confidentiality Agreement.

STATEMENT OF FACTS

A. Home Market Foods, Inc.'s Business.

8. HMF manufactures, markets, and sells fully cooked protein specialty foods to both retail and food-service providers. HMF has a number of its own brands, including: (i) **Cooked Perfect®** (fully cooked fresh and frozen meatballs, fire grilled chicken, and chicken bites); (ii) **RollerBites®** (chicken, beef, and pork rolled snacks); **Bahama Mama®** (premium sausages and frankfurters); and **Eisenberg®** (premium frankfurters and gourmet sausage) ("**HMF Brands**"). HMF Brands are sold to retailers—such as BigY, BJ's, Market Basket, Hannaford, Shaws, Stop & Shop, Target, Wal-Mart, and Wegmans—who then sell HMF's products to consumers.

9. HMF also has a private label business whereby it manufactures and distributes products that are sold under a customer's own brand name subject to the unique requirements of each customer. A customer's product specifications and requirements are treated as highly confidential information by HMF.

10. The industry in which HMF operates is referred to as the "Consumer Packaged Goods" ("**CPG**") industry. The CPG industry involves the sale of items used daily by consumers that require routine replacement or replenishment, such as the specialty foods manufactured and sold by HMF. Although consumer demand for food products generally remains constant, the

industry is highly competitive based on, among other things, high market saturation and relatively low consumer switching costs (i.e., the cost a consumer incurs by changing brands).

11. The specialty food product sector within the CPG industry is one of the most competitive sectors in the industry. Consequently, food manufacturers—like HMF—must continually position themselves to effectively compete for "shelf space" in retail stores. To do so, food manufacturers, such as HMF, implement a highly detailed and data-driven strategy that seeks to give them precise information to decide on what products should be sold to what retailers, in what geographic areas, and when. This includes knowing, among other things, how different retailers sell their products to consumers, what retailer customer bases will likely purchase and when, what distribution channel will be most efficient, and how to brand and price products for success.

12. To accomplish its business objectives, HMF creates, tracks, maintains, analyzes, and uses highly confidential data to develop its pricing, shipping, marketing, and distribution strategies for its private label and HMF Brands, as well as the pricing and product requirements of retailers through which those products are sold. This information, along with the strong relationships it has built with its customers, gives HMF a competitive advantage over others. Disclosure of this information to a competitor (or a customer) would irreparably harm the significant goodwill HMF has built in the industry over the last fifty (50) years and its ability to stay competitive in the marketplace. Indeed, armed with HMF's confidential information, a competitor could easily undercut HMF's pricing and promotion strategy and take shelf space away from HMF, or target retailers in particular areas to edge HMF out of the market altogether.

B. Mr. Lubow's Employment with HMF.

13. By letter dated June 25, 2012 ("**Offer Letter**"), HMF offered Mr. Lubow the position of Midwest Division Retail Sales Manager.

14. The offer made to Mr. Lubow was subject to a number of contingencies, including his execution of the Confidentiality Agreement.

15. Mr. Lubow accepted this offer and signed the Offer Letter on June 29, 2012. Attached hereto as **Exhibit A** is a genuine copy of the Offer Letter

16. Mr. Lubow's employment began with new hire orientation at the Company's headquarters in Massachusetts on July 23 and 24, 2012.

17. Mr. Lubow signed the Confidentiality Agreement during his new hire orientation on July 24, 2012. Attached hereto as **Exhibit B** is a genuine copy of the Confidentiality Agreement.

18. When Mr. Lubow signed the Confidentiality Agreement, Mr. Lubow acknowledged that he was an "at will" employee and that his employment was subject to termination by either the Company or Mr. Lubow at any time, with or without cause. *See* **Exhibit B**, Sec. 10(a).

19. By signing the Confidentiality Agreement, Mr. Lubow also agreed to maintain the confidentiality of HMF's Proprietary Information, both during his employment relationship and after it ended. *See* **Exhibit B**, Sec. 2(a), (b), and (c).

20. The Confidentiality Agreement provides, in pertinent part, as follows:

> I recognize that the Company owns, possesses or uses valuable trade secrets and confidential and proprietary information concerning the products, business and operations of the Company, including but not limited to valuable trade secrets and information related to research and development, product concepts and designs, products, product formulas and formulations, product recipes, product manufacturing and production processes and techniques, product packaging, finances, marketing, advertising, customers, customers lists, customer prospects, customer purchase requirements, sales projections, strategies and results, business plans and strategies (including but not limited to plans for new produce development), business ventures, combinations and collaborations, prospects for business ventures, combinations and collaborations, licensing and prospective licensing projects, trademarking and prospective trademarking projects (including but not limited to trade names and trademarks under consideration), suppliers, employees, and analyses and information regarding what product formulations, designs, recipes, concepts and manufacturing processes do

> and do not work, and including further the Developments. *See* **Exhibit B**, Sec. 2(a).

21. The definition of Proprietary Information in Section 2(a) of the Confidentiality Agreement includes certain customer information. Specifically, Section 2(a) provides that:

> I also understand that the Company from time to time has in its possession information which is claimed by others to be proprietary and which the Company has agreed to keep confidential. I agree that such information will be Proprietary Information for purposes of this Agreement. *See* **Exhibit B**, Sec. 2(a).

22. By signing the Confidentiality Agreement, Mr. Lubow agreed to hold the Company's Proprietary Information "in the strictest confidence" and acknowledged that his relationship with the Company is "one of high trust and confidence by reason of [his] access to and contact with the Proprietary Information." *See* **Exhibit B**, Sec. 2(b).

23. Mr. Lubow agreed that he would not "remove from the Company's premises Proprietary Information except where essential for [him] to carry out [his] duties in connection with [his] employment, and then only with the prior advance knowledge and permission of the Company." *See* **Exhibit B**, Sec. 2(c).

24. Mr. Lubow agreed that all Proprietary Information is the exclusive property of the Company and that:

> (a) upon termination of his work he would promptly deliver to the Company "all Proprietary Information and all computer programs, specifications, drawings, blueprints, data storage devices, notes, memoranda, notebooks, records, reports, files and other documents (and all copies or reproductions of such materials) in [his] possession or under [his] control, whether prepared by [him] or others, which contain Proprietary Information"; and
>
> (b) upon termination of his employment with the Company he would "return promptly all documents, extracts of documents, and other property and information belonging to the Company or its customers or business (whether or not any such matters are or contain Proprietary Information), including but not limited to all documents and information stored in electronic form or on any computer or other device (whether or not any such equipment is owned by the Company or located at any of its places of business)." *See* **Exhibit B**, Sec. 2(f) and 6.

25. Mr. Lubow further agreed that "to the extent that I have stored documents, extracts of documents or information in electronic form on computers or other devices not owned by the Company (which I understand and agree I may only do during my employment with prior permission of the Company) I shall permanently destroy all files and documents containing such material after forwarding electronic copies to the Company." *See* **Exhibit B**, Sec. 6.

26. Finally, by entering into the Confidentiality Agreement, Mr. Lubow expressly recognized and acknowledged as follows:

> I recognize and acknowledge that irreparable damages would be caused to the Company, and that monetary damages would not compensate the Company for its loss, should I breach the terms of this Agreement. Accordingly, in addition to all other remedies available to the Company at law or in equity, upon a showing by the Company that I have violated or am about to violate the terms of this Agreement, I hereby consent to the entry by a court of competent jurisdiction of an injunction or declaratory judgment, without the posting of any bond or other surety, enforcing the terms of this Agreement, including without limitation preventing disclosure or further disclosure by me of Proprietary Information. *See* **Exhibit B**, Sec. 9.

27. The Confidentiality Agreement provides that it is governed by the laws of the Commonwealth of Massachusetts, and that the parties agree that "the federal or state courts of the Commonwealth of Massachusetts shall have the exclusive jurisdiction and venue for any dispute under this Agreement. *"See* **Exhibit B**, Sec. 10(f).

28. In consideration of his employment with HMF, and the compensation and benefits paid to him, Mr. Lubow signed the Confidentiality Agreement thereby agreeing to be bound by its terms.

29. Also, when Mr. Lubow began his employment at HMF, he acknowledged his review and receipt of HMF's Employee Handbook, which includes policies regarding the Company's confidential information and protection of its data, and Mr. Lubow affixed his signature just below the Confidential Information Policy. A copy of the handbook acknowledgment, executed by Mr. Lubow on July 24, 2012, is attached hereto as **Exhibit C**.

30. HMF's Employee Handbook Confidential Information acknowledgment, as executed by Mr. Lubow, provides as follows:

> I am aware that during the course of my employment, confidential information may be made available to me (for instance, product designs, marketing strategies, customer lists, pricing policies and other related information). I understand that this information is proprietary and critical to the success of Home Market Foods, Inc. I agree not to use this information outside of the Company's premises or share this information with non-Company employees. In the event of termination of employment, whether voluntary or involuntary, I hereby agree not to utilize, share, or exploit this information with any other individual or company. *See* **Exhibit C**.

31. Based on Mr. Lubow's execution of the Offer Letter, Confidentiality Agreement and Employee Handbook Confidential Information acknowledgment, Mr. Lubow was given access to HMF's Proprietary Information and entrusted with the responsibility of maintaining its confidentiality.

C. HMF's Proprietary Information.

32. Among other things, HMF maintains the following Proprietary Information that Mr. Lubow had access to during his employment: customer shipment information, reflecting Company revenues per customer; financial information, including variable margins and customer pricing; strategic documents related to pricing and marketing methodologies, customer-specific products, recipes, and requirements; and highly sensitive information regarding sales and trade development.

33. In particular, unique pricing and promotion tactics, including how to address retailer margin requirements are critical components of HMF's overall sales and product-placement go-to-market strategy. HMF develops customer pricing using a proprietary methodology based on unique recipe requirements dictated by the customer, annual revenue and tonnage projections (i.e., "plant utilization"), and consideration of the customer's in-market pricing strategy, including targeted suggested retail price and known gross margin requirements. Also,

when making pricing decisions and developing sales and marketing strategies, HMF aggregates and uses confidential information relating to its products, business, and operations, including information about product concepts, recipes, and formulas. Similarly, HMF assesses targeted pricing adjustments on commodity market fluctuations and inflationary costs, which adjustments are determined based on unique formulas and methods. HMF also creates, maintains, aggregates, and analyzes shipping information for all of its customers, which also aides HMF in its pricing and sales strategies and methodologies. In addition, HMF prepares financial reports that directly impact its decisions regarding pricing and sales. One such document includes variable margin reports in which HMF compiles its unique information regarding sales and costs, broken down by customer in order to determine its profit percentages. All of this information is not available to HMF's competitors, cannot be obtained through public sources, and gives HMF a competitive advantage in the CPG industry.

34. HMF also maintains confidential and proprietary information about its customers, including customer purchase requirements, customer business plans and strategies, sales projections, and product development plans. For some customers, HMF is entrusted to manufacture food products using recipes that are unique to that customer and based on the customers specifications. This is proprietary information to both HMF and its customers that HMF is required to keep confidential.

D. HMF's Significant Efforts to Protect Its Proprietary Information.

35. Given its value and importance, HMF takes extensive measures to ensure the secrecy and to protect the security of its Proprietary Information within HMF and as to third parties, including competitors. These measures include, among other things, (i) mandatory confidentiality and non-disclosure agreements, (ii) network security, (iii) physical security, and (iv) company policies and procedures.

36. Confidentiality and Non-Disclosure Agreements. HMF protects its Proprietary Information by requiring all employees to sign a confidentiality and non-disclosure agreement like the Confidentiality Agreement Mr. Lubow. Employees must sign these agreements upon commencement of employment. Failure to do so will prevent hiring. By signing these agreements, HMF employees agree—like Mr. Lubow—not to disclose to others or use any Proprietary Information that is learned during their employment and to take "appropriate precautions to maintain the security of such information." HMF employees—like Mr. Lubow—also agree to return all Proprietary Information promptly upon termination of their employment.

37. Network Security. HMF uses encryption, firewalls, anti-virus/malware software, virtual private network ("**VPN**") access, two-step user authentication, passwords, and auto-locking software to protect its Proprietary Information.

38. HMF employees must take the following steps to access HMF's network: (1) enter their unique user log-in password; (2) enter their unique password to sign-in to the VPN; (3) follow two-step authentication process entering a Microsoft authentication code that is provided to the employee on a separate device (such as a mobile phone by way of text message, phone call or through a mobile phone application). HMF employees cannot access HMF's cloud applications or shared drives through the VPN until they have completed the two-step authentication process.

39. HMF also requires complex computer passwords factoring in password history and age requirements. Further, Next Generation Firewalls (a network security system that monitors and controls incoming and outgoing network traffic) are deployed, logs are sent to a Security Information and Event Management system (a system that collects data from a computer network in real time) with a managed Security Operation Center ("vSOC") (a third-party cybersecurity service) actively monitoring all network and firewall applications. Next Generation endpoint protection (sophisticated anti-virus software) and response solution is deployed on all "endpoints"

(i.e., a device physically connected to a network,) and is actively monitored by vSOC. Finally, encryption (Bitlocker) is enabled on all endpoints.

40. In addition to network protections, HMF also takes additional steps to protect and restrict access to folders and files that contain Proprietary Information. For example, documents containing certain financial information are only circulated on a need-to-know basis, and if sent by email, the document is password protected and the password is provided to the recipient by text message on a separate device. If saved to the HMF Shared Drive, these types of documents are placed in restricted folders that are only accessible to employees with permission.

41. HMF has dedicated substantial resources to protecting its Proprietary Information, including an annual spend of approximately $500,000 and $400,000 of capital investments. These costs cover the following security measures: a dedicated Cyber Security Analyst on staff; firewalls; VPN access; port security; Microsoft EM&S; vSOC managed Security Information and Event Management and endpoint security; and BitLocker encryption.

42. Physical Security. The Company prevents third persons from accessing its facilities by requiring that the facilities are secure and can be accessed only by the use of "prox cards" (electronic keys). In addition, HMF utilizes other security measures including security cameras, visitor sign in sheets, and locked drawers and filing cabinets. Digital records of bills of materials (documents reflecting the list of materials that go into a finished good, including recipes and packaging), costing, pricing, company financials, and formulations are hosted by on-premise servers located behind locked doors secured by an access control system that limits physical access.

43. Other Company Policies. In addition to the use of confidentiality and nondisclosure agreements, and the Employee Handbook Confidential Information acknowledgment referred to above in paragraphs 29 and 30, HMF's employee handbook contains two provisions regarding

confidential information which HMF employees are required to review and acknowledge receipt.

These sections provide:

i. Data Confidentiality. Employees often have access to confidential or proprietary information, such as data about employees, customers, vendors, contractors, or other individuals or entities that do business with HMF. Under no circumstances is it permissible for employees to disseminate any confidential information relating to those individuals. Do not disclose confidential financial data, or other non-public proprietary company information. Do not share confidential information regarding business partners, vendors, or customers. Misuse or unauthorized disclosure of confidential information not otherwise available to persons or firms outside HMF is cause for disciplinary action up to and including termination of employment. (Handbook, Sec. 6.11).

ii. Confidentiality and Non-Disclosure Statement. As a condition of employment, all employees are required to sign a Non-Disclosure, Inventions, Work-for-Hire, and Non-Competition Agreement. Company personnel should not discuss internal Company matters or developments with anyone outside the Company, except as required in the performance of the regular Company duties. **Information about products, marketing plans, cost, earnings and organizational charts are critical to the success of HMF and is confidential and proprietary**. Such information, including but not limited to purchase prices, processes and vendor information and other business, proprietary data should not be disclosed to other employees except as required in connection with the performance of their job. (Handbook, Sec. 6.12) (emphasis added).

44. Furthermore, all new employees are informed of their obligations to HMF regarding confidentiality and receive training regarding Company policies, including confidentiality.

45. HMF's employee handbook also provides the following policies pertaining to employee use of Company computers:

i. "Computer hardware and software provided to employees by the Company is the property of the Company. This includes...laptops..." (Handbook, Sec. 6.11)

ii. "It is unacceptable for any employee to use HMF's Information Technology Resources...for any of the following:...to gain or attempt to gain, unauthorized access to any computer or network; (Handbook, Sec. 6.11)

46. Moreover, when an HMF employee is terminated from employment , they are provided with a separation letter from HMF. Among other things, the separation letter reminds the employee to return Company property, and to continue protecting and not disclosing the Company's confidential and proprietary business information.

E. Mr. Lubow's Unlawful Conduct, including Unauthorized Access and Misappropriation of HMF's Proprietary Information.

47. In connection with his employment, Mr. Lubow was provided a Company owned laptop computer (serial no. 8JJTL32) ("**Old Laptop**") by HMF in June 2015 for purposes of carrying out his job duties on behalf of HMF.

48. In March 2018, Mr. Lubow was provided a replacement laptop computer (serial number D4L19H2) ("**New Laptop**"), which had the ability to connect to the internet. Upon receipt of the New Laptop, Mr. Lubow was instructed to return the Old Laptop. Mr. Lubow did not return the Old Laptop and maintained possession of both Company laptops.

49. At all times, the laptops provided to Mr. Lubow by HMF remained the property of HMF.

50. On September 23, 2020, Mr. Lubow was notified that his employment would be terminated effective September 25, 2020.

51. On September 23, 2020, HMF representatives spoke with Mr. Lubow to inform him of his termination and asked him to return all Company property, as he was no longer authorized to access it.

52. Following that meeting, Mr. Lubow was provided a letter, dated September 23, 2020, regarding details of his employment separation. A true copy of the September 23, 2020 separation letter is attached as **Exhibit D**.

53. The September 23rd separation letter specifically reminded Mr. Lubow to promptly return all Company property, and "to leave intact all electronic Company documents on the Company's systems."

54. The September 23rd separation letter also reminded Mr. Lubow of his "continuing strict legal obligations to protect and not to disclose the Company's confidential and proprietary business information which you acquired during the course of your employment."

55. On or about October 6, 2020, Mr. Lubow returned the Old Laptop to HMF.

56. Upon realizing that Mr. Lubow still had a Company laptop in his possession (i.e., the New Laptop), by letter dated October 14, 2020, counsel for HMF reminded Mr. Lubow's counsel of his client's responsibility to return all Company property, specifically requesting that Mr. Lubow promptly return the New Laptop. On October 15, 2020, HMF's Vice President of Human Resources emailed Mr. Lubow directly, stating that "the laptop with serial number D4L19H2 was issued to you, and we have not received that laptop. I ask that nothing be downloaded from the laptop as the hardware as well as everything on the laptop is company property."

57. Mr. Lubow returned the New Laptop to HMF on October 30, 2020.

58. Mr. Lubow's significant delay in returning HMF's laptops and his deliberate decision to keep the New Laptop for a substantial period of time raised red flags for HMF.

59. Upon receipt of Mr. Lubow's New Laptop, and upon the advice of counsel, HMF immediately sent the New Laptop to StoneTurn Group, LLP ("**StoneTurn")** to conduct a forensic examination. Attached hereto as **Exhibit E**, is the Declaration of Daniel R. Fuller, including attached **Exhibits 1 and 2** (referred to herein as "ex.").

60. What HMF uncovered during from the investigation conducted by StoneTurn (which is still ongoing) is simply remarkable and demonstrates Mr. Lubow's brazen unlawful conduct.

61. In spite of his obligations under the Confidentiality Agreement, HMF's policies, and the express instructions provided to Mr. Lubow prior to and after his date of termination, Mr. Lubow repeatedly accessed the New Laptop, including HMF's Proprietary Information.

62. In particular, between the time period when Mr. Lubow was notified of his termination, September 23, 2020, and the date that HMF received the New Laptop, October 30, 2020, Mr. Lubow accessed the New Laptop on twenty (20) different days.

63. During this same time, Mr. Lubow connected seven (7) different USB drives to the New Laptop as follows:

Device Name	USB Serial Number	First Connection	Last Connection
OSCOO USB USB Device	6&13f06b7a&0	09/27/2020 04:29:42 AM	10/26/2020 01:40:28 PM
V88 V88 USB Device	261007018663C200	07/11/2020 02:47:42 PM	10/23/2020 09:18:50 AM
USB DISK 3.0 USB Device	070002CD0251F161	10/17/2020 01:16:06 AM	10/17/2020 07:07:59 AM
USB DISK 3.0 USB Device	070001B2162A3987	10/16/2020 11:27:30 PM	10/16/2020 11:27:29 PM
OSCOO USB USB Device	6&136bad5&0	09/24/2020 06:07:31 AM	10/15/2020 07:57:38 AM
USB Device	11042858004371	10/11/2020 07:31:09 PM	10/11/2020 07:31:08 PM
OSCOO USB USB Device	6&26aa1c1f&0	10/03/2020 05:09:43 AM	10/09/2020 10:47:39 AM

See **Exhibit E**, ¶ 8, ex. 2.

64. Of the seven (7) USB drive connections, five (5) USB devices were connected to the New Laptop, after Mr. Lubow was specifically requested, by letter to his counsel (October 14, 2020) and by email to him directly (October 15, 2020), to return the New Laptop and to not download anything from the laptop. None of the USB devices identified in the above chart were returned to HMF by Mr. Lubow. *See* **Exhibit E**, ¶ 8, ex. 2.

65. Upon information and belief, Mr. Lubow is still in possession of the aforementioned USB devices.

66. Through the forensic analysis, HMF also discovered that Mr. Lubow opened and viewed over one-hundred documents that were stored both on the HMF New Laptop and on the USB drives. StoneTurn established this information by reviewing "LNK files." When a document is opened through Windows Explorer, a LNK file, unique to that individual file or document, may be stored to allow a user to quickly access that file in the future from a recent items list. *See* **Exhibit E**, ¶ 9. LNK files store the path of the target file as well as other associated metadata. *See* **Exhibit E**, ¶ 9. The Last Written date of a LNK file identifies the most recent date that the target file or folder was opened. *See* **Exhibit E**, ¶ 9.

67. By reviewing the file names that were accessed from the USB drives connected to the New Laptop and comparing them to documents in HMF's possession, HMF has determined that Mr. Lubow accessed and, on information and belief, has copies of HMF's Proprietary Information on his personal USB devices. By way of example (and by no means intending to be all inclusive) there are:

A. File containing customer shipment information in the Central West territory for 2019 and 2020. This file is used to provide sales leaders and business leaders with shipment status by customer, and reflects product, pricing and revenue information broken down by customer. This information is created by HMF and is used to address business opportunities where deficits are identified.

B. File containing customer's internal strategy review. This file is created by HMF using HMF and customer proprietary information. It is a key tool of HMF's business development, and involves an in depth review of a customer's relationship, including a three year growth plan, targeted financials and product ideas.

C. File containing customer specific information including store counts, and pricing by SKU produced for a specific customer. HMF creates a report with this information to understand key business trends of the customer, including sales forecasting, pricing issues, and distribution gaps.

D. Files containing confidential information regarding customer-specific pricing and promotion strategies. This information is used to justify pricing actions with various customers.

E. Files containing planning information broken down by customer and brand sales information, including actuals, and year-end projections. These files contain sensitive brand and customer specific information, upside activity identification, and financial impact information.

F. Files reflecting variable margin information broken down by customer. This information is used by sales leaders to address opportunities. HMF creates these reports by compiling its unique information regarding sales and costs, broken down by customer in order to determine its profit percentages. This information directly impacts HMF's decision-making when it comes to adjusting customer pricing, and is therefore highly sensitive information.

G. Customer price lists which are specific to unique SKUs produced exclusively by HMF for a customer. These files include pricing information and customer terms specific to the HMF relationship.

As noted above, HMF is continuing its investigation and is still in the process of reviewing all of the information provided by StoneTurn. The list above merely provides examples of types of files that Mr. Lubow accessed on the New Laptop and through the USB drives which contained HMF's Proprietary Information.

68. Further, on September 24, 2020—the day after Mr. Lubow was notified of his termination—HMF received an email from Mr. Lubow's personal email address to his HMF email account that contained two attachments that, on information and belief, were created by Mr. Lubow and contain HMF's Proprietary Information. One of the email attachments entitled "HMF 2020 8AM.docx" included the following statement (emphasis added):

"I have entire PPT with pricing by customer for the entire company from 6/26/20."

The referenced pricing PowerPoint (PPT) contains Proprietary Information regarding customer specific pricing, including pricing increases and margin information.

69. The Proprietary Information contained within the HMF files accessed and, upon information and belief, copied by Mr. Lubow to his USB drives, is a vital source of HMF's competitive advantage.

70. Unquestionably, Mr. Lubow used improper means (breach of his Confidentiality

Agreement and breach of HMF polices, in particular) to maliciously access HMF's Proprietary Information without HMF's consent and without authorization after his employment had been terminated. On information and belief, Mr. Lubow then copied HMF's Proprietary Information to one or more USB drives and has since maintained it for his own use.

71. HMF believes that Mr. Lubow intends to disclose HMF's Proprietary Information to others, or use the information for himself—all to HMF's severe detriment—based on, among other things, the following actions taken by Mr. Lubow after his termination of employment and after he was instructed to return all HMF Proprietary Information and property:

i. using the New Laptop within twenty-four (24) hours of his termination after being instructed to return it to HMF;

ii. accessing the New Laptop on twenty (20) different days between September 23, 2020 and October 26, 2020;

iii. viewing over a hundred documents containing HMF Proprietary Information on the New Laptop;

iv. inserting seven different USB devices into the New Laptop that contained HMF Proprietary Information;

v. deciding to return only one of two HMF's laptops in his possession, and failing to return the second Laptop until more than two weeks after he was reminded to do so by HMF on October 14, 2020;

vi. continuing to access the New Laptop and insert multiple USB devices that contained HMF Proprietary Information into the New Laptop after he was reminded again by HMF on October 15, 2020 not to download any information from the New Laptop;

vii. sending an email to his HMF email account with attachments that appear to have been created by Mr. Lubow and contain references to HMF's Proprietary Information, and stating he has a copy a PowerPoint with the "entire PPT with pricing by customer for the entire company from 6/26/20."

Put simply, there is no other reasonable inference and conclusion that may be derived from Mr. Lubow's aberrant conduct.

F. Imminent, Irreparable Harm to HMF.

72. Mr. Lubow's actions prevent HMF from effectively managing the risk associated with Mr. Lubow's unauthorized possession of HMF's Proprietary Information.

73. Without access to the seven USB devices that Mr. Lubow inserted into the New Laptop following his termination of employment, HMF has no way of knowing the full extent of what Proprietary Information Mr. Lubow has taken and may use.

74. The protection of HMF's Proprietary Information is critically important to HMF. If HMF's confidential and Proprietary Information (including its confidential and proprietary sales, pricing, customer, shipment, marketing, strategic and financial information) was disclosed to Mr. Lubow's new employer or other third party, HMF's competitors could immediately learn HMF's sales volumes, profit margins, and sophisticated pricing and sales strategies that took many years to refine for key customers—causing irreparable harm to HMF. Specifically, a competitor could use the confidential and Proprietary Information to undermine HMF's sales efforts by undercutting HMF's pricing, unfairly competing with HMF for business with its customers, and potentially resulting in enormous financial loss to HMF totaling over tens of millions of dollars.

75. Further, because HMF's sales, pricing, shipment, marketing and strategic information for each customer is confidential and proprietary, the disclosure of such customer information to other customers or competitors would cause irreparable harm to HMF's customer relationships and goodwill that it has worked hard to create and develop.

76. There is of course significant economic value to maintaining the secrecy of HMF's Proprietary Information, which is one of the main reasons that HMF has developed company policies, implemented physical and electronic security measures, and required employees, such as Mr. Lubow, to sign a confidentiality and non-disclosure agreement, in order to protect its Proprietary Information.

77. By signing the Confidentiality Agreement, Mr. Lubow acknowledged that "irreparable damages" would be caused to the Company if he breached the terms of the Confidentiality Agreement. *See* **Exhibit B**, Section 9.

CLAIMS FOR RELIEF

COUNT I

(Breach of Contract)

78. HMF incorporates each of the foregoing paragraphs in their entirety as if specifically set forth herein.

79. Mr. Lubow was offered employment by HMF on or about June 25, 2012.

80. In consideration of his employment with HMF, and the compensation and benefits paid to him, on July 24, 2012, Mr. Lubow signed the Confidentiality Agreement thereby agreeing to be bound by its terms.

81. HMF and Mr. Lubow are parties to the Confidentiality Agreement which is an enforceable contract governed by Massachusetts law.

82. Pursuant to the Confidentiality Agreement, among other things, Mr. Lubow agreed to hold the Proprietary Information in "strictest confidence" and not to disclose or use it for his own benefit, the benefit of others or to the detriment of the Company.

83. Mr. Lubow agreed to be bound by the terms of the Confidentiality Agreement and maintain the confidentiality of HMF's Proprietary Information during and after his employment.

84. Mr. Lubow agreed not to remove Proprietary Information except in connection with carrying out his duties and with the advance knowledge and permission of the Company.

85. Mr. Lubow agreed to return all Proprietary Information to the Company upon termination of employment.

86. Mr. Lubow breached the Confidentiality Agreement by repeatedly accessing the New Laptop without authorization after the termination of his employment.

87. Mr. Lubow breached the Confidentiality Agreement by repeatedly accessing HMF Proprietary Information without authorization after the termination of his employment.

88. Mr. Lubow breached the Confidentiality Agreement by accessing HMF Proprietary Information on USB devices that remain in his possession, custody, or control, and/or were not given to HMF after the termination of his employment.

89. Mr. Lubow breached the Confidentiality Agreement by, on information and belief, copying the HMF's Proprietary Information from the New Laptop to USB devices with the clear intent to misappropriate it.

90. HMF fully performed all of its obligations under the Confidentiality Agreement.

91. Mr. Lubow's conduct, as described above, has breached and threatens to continue to breach the Confidentiality Agreement.

92. As a result of Mr. Lubow's breaches of contract, HMF has been harmed and faces further irreparable harm. HMF's remedy at law is inadequate to compensate it for the harm Mr. Lubow has done. HMF therefore seeks temporary, preliminary, and permanent injunctive relief to recover and protect its confidential and proprietary information, and trade secrets, as well as to protect other legitimate business interests.

COUNT II

(Breach of Implied Covenant of Good Faith and Fair Dealing)

93. HMF incorporates each of the foregoing paragraphs in their entirety as if specifically set forth herein.

94. On July 24, 2012, Mr. Lubow signed the Confidentiality Agreement.

95. The Confidentiality Agreement is valid and legally binding, and is governed by Massachusetts law.

96. There exists an implied covenant of good faith and fair dealing in every contract, including the Confidentiality Agreement signed by Mr. Lubow.

97. Following Mr. Lubow's termination of employment from HMF, Mr. Lubow breached the implied covenant of good faith and fair dealing.

98. Mr. Lubow breached the Confidentiality Agreement's implied covenant of good faith and fair dealing by repeatedly accessing the New Laptop without authorization after the termination of his employment.

99. Mr. Lubow breached the Confidentiality Agreement's implied covenant of good faith and fair dealing by repeatedly accessing HMF Proprietary Information without authorization after the termination of his employment.

100. Mr. Lubow breached the Confidentiality Agreement's implied covenant of good faith and fair dealing by accessing HMF Proprietary Information on USB devices that remain in his possession, custody, or control, and/or were not given to HMF after the termination of his employment.

101. Mr. Lubow breached the Confidentiality Agreement's implied covenant of good faith and fair dealing by, on information and belief, copying the HMF's Proprietary Information from the New Laptop to USB devices with the clear intent to misappropriate it.

102. Furthermore, it is more than reasonable to infer and conclude that Mr. Lubow took these actions in bad faith to secure Proprietary Information for himself and to use it to benefit himself and his future employer.

103. As a result of Mr. Lubow's breaches of the implied covenant of good faith and fair dealing, HMF has been harmed and faces irreparable harm. HMF's remedy at law is inadequate to compensate it for the harm Mr. Lubow has done. HMF therefore seeks temporary, preliminary, and permanent injunctive relief to recover and protect its confidential and proprietary information, and trade secrets, as well as to protect other legitimate business interests.

COUNT III

(Misappropriation of Confidential Information)

104. HMF incorporates each of the foregoing paragraphs in their entirety as if specifically set forth herein.

105. Mr. Lubow was entrusted with HMF's Proprietary Information related to, among other things, its customers, pricing, and marketing.

106. HMF has taken reasonable steps to protect its Proprietary Information, including its trade secrets and confidential information.

107. Mr. Lubow had a duty not to disclose, use, or possess HMF's Proprietary Information without HMF's permission, while working for HMF and continues to have that duty after termination of his employment.

108. Upon information and belief, Mr. Lubow has misappropriated HMF's Proprietary information for his own use and personal gain.

109. As a result of Mr. Lubow's misappropriation, HMF has suffered and continues to be threatened with irreparable harm. HMF's remedy at law is inadequate to compensate it for the harm Mr. Lubow has done. HMF therefore seeks temporary, preliminary, and permanent injunctive relief to recover and protect its confidential and proprietary information, and trade secrets, as well as to protect other legitimate business interests.

COUNT IV

(Misappropriation of Trade Secrets in Violation of Massachusetts Trade Secrets Act, M.G.L. c. 93, §§ 42-42G)

110. HMF incorporates each of the foregoing paragraphs in their entirety as if specifically set forth herein.

111. As set forth above, HMF maintains various trade secrets as defined by M.G.L. c. 93, § 42(4), which HMF has taken reasonable steps to protect .

112. As set forth above, Mr. Lubow misappropriated those trade secrets as defined by M.G.L. c. 93, § 42(2).

113. Pursuant to M.G.L. c. 93, § 42A, HMF is entitled to enjoin Mr. Lubow's actual or threatened use of HMF's trade secrets.

114. HMF has been damaged by Mr. Lubow's misappropriation, including, without limitation, by having to retain counsel to protect HMF's trade secrets.

115. On information and belief, Mr. Lubow acted willfully and maliciously, which entitles HMF to an award of exemplary damages under M.G.L. c. 93, § 42B.

116. HMF is entitled to an award of its reasonable attorney's fees and costs pursuant to M.G.L. c. 93 § 42C.

117. As a result of Mr. Lubow's violation of the Massachusetts Trade Secrets Act and his willful and malicious acts, HMF is entitled to injunctive relief, exemplary damages, and an award of reasonable attorney's fees and costs.

COUNT V

(Violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

118. HMF incorporates each of the foregoing paragraphs in their entirety as if specifically set forth herein.

119. HMF's computer system is a protected computer network which is used across state lines in interstate commerce, has Internet access across state lines, and is used to transfer HMF information for sales in interstate commerce.

120. At the time of his termination Mr. Lubow was still in possession of two HMF laptop computers that had been issued to him for his work-related use.

121. Because his employment with HMF was terminated, Mr. Lubow was no longer authorized to access the HMF laptops or the information and data contained therein.

122. Notwithstanding this lack of authorization, and upon information and belief, Mr. Lubow repeatedly accessed the New Laptop, viewed HMF's Proprietary Information on the New Laptop, and after his termination, inserted seven USB drives into the New Laptop which contained HMF's Proprietary Information, and upon information and belief, this was done to obtain information from HMF's protected computer.

123. Through these actions, Mr. Lubow has:

i. Intentionally accessed a computer without authorization or exceeded his authority to obtain information from a protected computer in violation of 18 U.S.C. § 1030(a)(2)(C);

ii. Intentionally accessed a protected computer without authorization, and as a result of such conduct, recklessly caused damage and loss in violation of 18 U.S.C. § 1030(a)(5)(B) and (C);

124. The filing of this claim is proper under 18 U.S.C. § 1030(g) and 18 U.S.C. § 1030(c)(4)(A)(i)(I) because Mr. Lubow's conduct described above has caused loss to HMF in excess of $5,000, including costs associated with responding to Mr. Lubow's misappropriation, costs of conducting a forensic examination, and costs of conducting a damage assessment in order to respond to Mr. Lubow's offenses.

125. As a result of Mr. Lubow's violation of the Computer Fraud and Abuse Act, HMF is entitled to injunctive relief and compensatory damages.

PRAYERS FOR RELIEF

WHEREFORE, HMF respectfully requests that the Court take affirmative steps to prevent Mr. Lubow from using and destroying HMF's Proprietary Information, and requiring Mr. Lubow to return the Proprietary Information, including by ordering the following temporary, preliminary, and permanent injunctive and equitable relief:

1. Preventing Mr. Lubow and any person or entity acting on his behalf or in concert with him, from destroying any evidence, tangible or electronically stored, that is the subject matter of this proceeding, including the universal serial bus ("**USB**") devices and any other devices or data sources in Mr. Lubow's possession, custody, or control that may contain any "Proprietary Information" as that term is defined in Mr. Lubow's Non-Disclosure, Inventions, Work-For-Hire and Non-Competition Agreement, dated July 24, 2012, as attached as Exhibit B to HMF's Verified Complaint for Injunctive and Equitable Relief;

2. Preventing Mr. Lubow and any person or entity acting on his behalf or in concert with him, from disclosing or copying any Proprietary Information, including the information contained on the USB devices and any other devices or data sources in Mr. Lubow's possession, custody, or control that may contain any Proprietary Information, to any third-party except for Mr. Lubow's counsel or a court of competent jurisdiction.

3. Requiring Mr. Lubow to surrender the USB devices and any other storage devices or data sources in Mr. Lubow's possession, custody, or control that may contain HMF's Proprietary Information for forensic copying by HMF's forensics expert;

4. Awarding exemplary damages and compensatory damages, in accordance with G.L. c. 93, § 42B;

5. Awarding attorneys' fees and costs incurred; and

6. For such other and further relief as the Court may deem just and proper.

Dated: December 8, 2020

HOME MARKET FOODS, INC.,

By its attorneys,

/s/ Terence P. McCourt
Terence P. McCourt (BBO# 555784)
David G. Thomas (BBO# 640854)
Amanda L. Carney (BBO# 694503)
Greenberg Traurig, LLP
One International Place, Suite 2000
Boston, MA 02110
Tel: (617) 310-6000
Fax: (617) 310-6001
mccourtt@gtlaw.com
thomasda@gtlaw.com
carneya@gtlaw.com

JURY TRIAL DEMANDED

HMF respectfully demands a trial by jury on all matters so triable.

VERIFICATION

VERIFICATION

I, Michael Weiermiller, state as follows:

1. I am the Senior Vice President of Sales & Marketing for Home Market Foods, Inc. ("HMF").

2. I have reviewed the above Verified Complaint and declare under penalty of perjury that the allegations of which (i) I have personal knowledge, I know or believe them to be true, and (ii) I do not have personal knowledge, I believe them to be true based on HMF's business records and/or the collective knowledge of HMF's employees.

Executed in Norwood, Massachusetts on December 12/8/20

Michael Weiermiller